

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----- X

IN THE MATTER OF AN APPLICATION FOR A
SEARCH WARRANT FOR:

THE ITEM KNOWN AND DESCRIBED AS: ONE
MOTOROLA XT1565 DROID MAXX2 CELLULAR
PHONE SERIAL NUMBER 990006240909332

----- X

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR A SEARCH
WARRANT

16M815

EASTERN DISTRICT OF NEW YORK, SS:

Leslie Adamczyk, being duly sworn, deposes and states that she is a Special Agent with the Federal Bureau of Investigation ("FBI"), duly appointed according to law and acting as such.

The source of your deponent's information and the grounds for her belief are as follows:¹

1. I have been a Special Agent with the FBI since August 2012 and am currently assigned to the New York Office. Since October 2014, I have been assigned to a Crimes Against Children squad and have investigated violations of criminal law relating to the sexual exploitation of children. I have gained expertise in this area through classroom training and daily work conducting these types of investigations. As a result of my training and experience, I am familiar with the techniques and methods used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities. As part of my responsibilities, I have been involved in the investigation of numerous child pornography ("CP") cases and have reviewed thousands of photographs depicting minors (less than eighteen years of age) being sexually exploited by adults. Through my experience in these

¹ Because this affidavit is submitted for the limited purpose of establishing probable cause for a search warrant, I have not set forth each and every fact learned during the course of the investigation.

investigations, I have become familiar with methods of determining whether a child is a minor. I am also a member of the Eastern District of New York Project Safe Childhood Task Force.

2. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from: my own personal participation in the investigation, my review of documents, my training and experience, and discussions I have had with other law enforcement personnel concerning the creation, distribution, and proliferation of CP. Additionally, statements attributable to individuals herein are set forth in sum and substance and in part.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

3. The property to be searched is ONE MOTOROLA XT1565 DROID MAXX2 CELLULAR TELEPHONE SERIAL NUMBER 990006240909332 seized during the course of an arrest of BLAISE CAROLEO (the "SUBJECT DEVICE").

4. The applied-for warrant would authorize the forensic examination of the SUBJECT DEVICE for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

5. On February 24, 2016, officers with the New York City Police Department arrested BLAISE CAROLEO for assaulting a New York City Bus Driver. Officers seized the SUBJECT DEVICE incident to CAROLEO'S arrest in New York County. CAROLEO advised the arresting officer and an Assistant Manhattan District Attorney ("ADA") that CAROLEO had a video of the alleged assault on the SUBJECT DEVICE. According to the ADA, CAROLEO showed the arresting officer the video and as a result the arresting officer seized it. On August 15, 2016, CAROLEO signed a "Consent to Search Form" allowing NYPD and the MANHATTAN DISTRICT ATTORNEY'S OFFICE to search the SUBJECT DEVICE. CAROLEO lives in Staten Island, New York. Data retrieved by the DA's Office from the SUBJECT DEVICE shows that CAROLEO used the SUBJECT DEVICE within the Eastern District of New York.

6. The SUBJECT DEVICE was searched by an investigator employed by the Manhattan District Attorney's Office ("DA's Office"). During the course of the search of the SUBJECT DEVICE, the investigator discovered multiple files of child pornography. One of the images depicts an approximately six-year-old female lying on her back with her legs spread open exposing her vagina and anus. In addition to the files of child pornography, the investigator discovered multiple Kik Messenger Chats between CAROLEO and numerous underage girls. Throughout the course of the various chats, the underage girls informed CAROLEO of their ages. During these chats, CAROLEO directed the underage girls to take sexually explicit

photographs of themselves. The underage females then sent the explicit photographs to CAROLEO. One underage female sent close-up images of her vagina. In the images, the underage female is digitally penetrating herself.

7. As noted above, the SUBJECT DEVICE was seized by the NYPD during the course of CAROLEO'S arrest in February 2016. The SUBJECT DEVICE was then turned over to the DA's Office after CAROLEO consented to a search of the SUBJECT DEVICE. Since the time of its seizure, the SUBJECT DEVICE remained in the possession of the NYPD and the DA's Office. The DA's Office subsequently agreed to give the SUBJECT DEVICE to the FBI so that the FBI may conduct further forensic examinations of the devices in support of potential federal charges. The SUBJECT DEVICE is currently in FBI custody in the Eastern District of New York.

TECHNICAL TERMS

8. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. "Chat" refers to any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.
- b. "Child Pornography," as used herein, is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction

involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

- c. “Computer,” as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”
- d. “Computer Server” or “Server,” as used herein, is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user’s computer via the Internet. A domain name system (“DNS”) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol (“IP”) address so the computer hosting the web site may be located, and the DNS server provides this function.
- e. “Computer hardware,” as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-

processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

- f. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- g. “Computer-related documentation,” as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- h. “Computer passwords, pass-phrases and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that

creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

- i. “Hyperlink” refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.
- j. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- k. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (“DSL”) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an “e-mail address,” an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can

establish communication with an Internet Service Provider (“ISP”) over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

- l. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.
- m. “Minor” means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).
- n. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (“DVDs”), Personal Digital Assistants (“PDAs”), Multi Media Cards (“MMCs”), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic

dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

- o. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).
- p. “URL” is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.
- q. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).
- r. “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (“HTML”) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (“HTTP”);

9. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at Motorola.com, I know that the SUBJECT DEVICE has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

10. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensic tools. Furthermore, photographs can be stored on electronic devices for many years. There is probable cause to believe that things that were once stored on the SUBJECT DEVICE may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

11. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT DEVICE because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may

depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

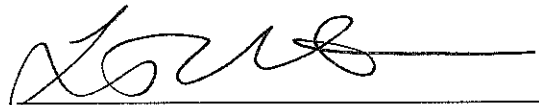
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to produce child pornography, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

12. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

13. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

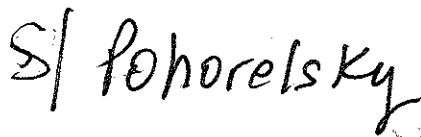
CONCLUSION

14. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the SUBJECT DEVICE described in Attachment A to seek the items described in Attachment B.



Leslie Adamczyk
Special Agent
Federal Bureau of Investigation

Sworn to before me this
9th day of September, 2016.



UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK